**CSCI 497 Senior Project Design Proposal**

**Name:** Matthew Tyler Poor

**Degree and Major:** Bachelor of Science in Cybersecurity

**Project Advisor Name:** Julie Henderson

**Expected Graduation Date:** May 2022

**Problem Statement:**

At the heart of cyber security is the ability to protect data while at-rest, in-transit, or in-use. The protection this data and information is needed by all government, companies, and individuals throughout the world. Therefore, it is crucial that management and government entities prioritize the mitigation of vulnerabilities among their networks and assets.

Thanks to penetration testers and red-team specialists, companies and governments can effectively close all risk related to vulnerabilities that are specific to their situation; furthermore, this will allow the company or government to better protect the confidentiality, availability, and integrity of all data and its assets. Penetration testing also allows companies and governments to be able to ensure that none of their critical or proprietary information is stolen, alleviating the probability of monetary loss or reputational loss. As a solution to information security needs, I will conduct a mock penetration test using a zero-day exploit that will allow me to gain initial access to a system, enumerate the network, escalate user privileges, and then gain control of the system. Afterwards, I will walkthrough detail remediation steps regarding the penetration testing methods and demonstration why they are important for data security to all company and governmental assets.

**Project Description:**

The project will consist of the creation of a virtual lab environment, using active directory. After this, I will create a zero-day exploit using the Python language that will act as my initial exploit. Next, I will access a basic user machine using the exploit and then enumerate the network to find other avenues of pivoting. After pivoting, I will then access an administrator account using privilege escalation techniques. Then, I will go through multiple different methods of hardening the network and ways of mitigating the vectors of attack. Finally, I will create a security tool that will automate the process of fixing a vulnerability.

**Proposed Implementation Languages:**

Bash

Python 3.0

PowerShell

**Libraries, Packages, Development Kits, etc. to be used in in the proposed implementation languages(s):**

Python Imports: Sys, Socket (For Buffer Overflow Exploit)

Use Gedit in Kali Linux to develop Buffer Overflow Exploit

Test Using Immunity Debugger and Vuln server, as well as Active Directory Envrionment

**Additional Software/Equipment Needed:**

VMWare Virtual Machines

Windows License

Kali Linux VM

**Personal Motivation:**

Since after college, I want to become a Penetration Tester and eventually start my own company doing this, this concept and project is extremely important to me. These concepts will be ones that I use every day in my future! Not only this, but the remediation steps and insight on how to fix these issues will be the biggest motivation for what I do. In helping people better secure their networks, systems, and assets I will be able to be a representative for Christ in the technical world.

**Outline of Future Research Efforts:**

Exploit will be submitted through GitHub.

The report will be created via a Microsoft Word Document.

Security tool will be submitted through GitHub and made public for everyday users.

A video will be created walking through the entire process.

**Schedule:**

**October 8th – Virtual Environment Created and Computers joined to Domain Controller**

* Build Windows Machines in a Virtual and Environment With Default Settings

**October 13th – Active Directory Environment Created**

* Users, Local Admins, Domain-Admins, Service Accounts
* Passwords

**October 15th – Exploit Created**

* Using python to write a buffer overflow exploit
* Testing exploit to ensure it works
* Documents failures

**October 22nd – Initial Access to the Network**

* Scanning techniques to discover devices on the internal network
* Pick our target
* Test gaining access to the network with the buffer overflow exploit
* Compromise a user account and look to pivot

**October 29th – Pivot/Privilege Escalation Techniques**

* Go through Active Directory exploits to escalate privileges
  + Bloodhound
  + SMB Relay Attacks
  + LLMNR Poisoning
  + IPv6 Man-In-The-Middle Attacks
  + Capturing Hashes
  + Hash Cracking
  + Brute Forcing
  + PowerShell Exploits
  + Hash Dumping
  + Pass The Hash Attacks
  + Token Impersonation
  + Exploiting Kerberos

**November 5th – Domain Controller Access / Admin Access**

* Gain control of Domain Admin Account
* Pivot to Domain Controller and Compromise the Entire Network
* Show the Dangers of a Compromised Network

**November 12th – Formal Penetration Test Report with Detailed Findings**

* Write Formal Penetration Test, Documenting Findings
* Detailed Remediation Steps for each finding
* Label Vulnerabilities in the network based off of NIST standards.

**November 19th – Full Remediation List with Steps**

* Full Remediation Steps and Demonstration
* Walkthrough Remediation Steps for Each Exploit Used During the Demonstration

**December 10th – Security Tool Created that Automates Remediation Steps**

* Create a Security Tool Using PowerShell to Automate Steps in the Remediation Process.